(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2005 (28.04.2005)

PCT

(10) International Publication Number
WO 2005/038634 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/IB2004/002710

(22) International Filing Date: 20 August 2004 (20.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03405749.7 17 October 2003 (17.10.2003) EP

(71) Applicant *(for all designated States except US)*: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: CAMENISCH, Jan [CH/CH]; Bahnhofstrasse 13, CH-8803 Rueschlikon (CH).

(74) Agents: TOLETI, Martin et al.; IBM Research GmbH, Zurich Research Laboratory, Saeumerstrasse 4 / Postfach, CH-8803 Rueschlikon (CH).

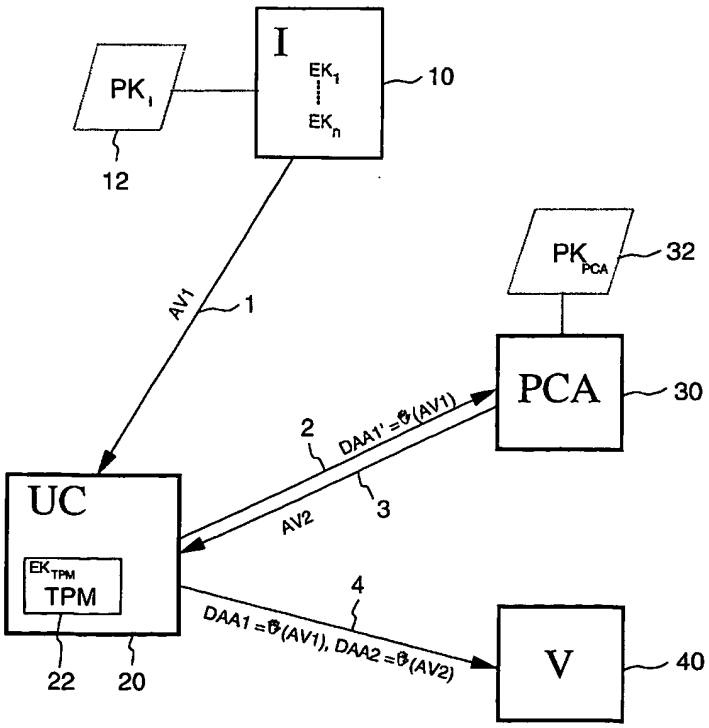
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: MAINTAINING PRIVACY FOR TRANSACTIONS PERFORMABLE BY A USER DEVICE HAVING A SECURITY MODULE



(57) Abstract: The present invention discloses a method and system for maintaining privacy for transactions performable by a user device having a security module with a privacy certification authority and a verifier. The system comprises an issuer providing an issuer public key PKI; a user device having a security module for generating a first set of attestation-signature values DAA1; a privacy certification authority computer for providing an authority public key PKPCA and issuing second attestation values AV2; and a verification computer for checking the validity of the first set of attestation-signature values DAA1 with the issuer public key PKI and the validity of a second set of attestation-signature values DAA2 with the authority public key PKPCA, the second set of attestation-signature values DAA2 being derivable by the user device 20 from the second attestation values AV2, wherein it is verifiable that the two sets of attestation-signature values DAA1, DAA2 relate to the user device.

WO 2005/038634 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.